

Approved:



KEVIN MEAD / MICAH FERGENSON
Assistant United States Attorneys

Before:

THE HONORABLE JAMES L. COTT
United States Magistrate Judge
Southern District of New York

23 MAG 3947

----- X
UNITED STATES OF AMERICA

: **COMPLAINT**

- v. -

: Violations of
18 U.S.C. §§ 371, 1030, 1349, 1343,
: 1028A, and 2

JOSEPH GARRISON,

Defendant.

: COUNTY OF OFFENSE:
NEW YORK
----- X

SOUTHERN DISTRICT OF NEW YORK, ss.:

MICHAEL GASSERT, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), and charges as follows:

COUNT ONE
(Conspiracy to Commit Computer Intrusions)

1. In or about November 2022, in the Southern District of New York and elsewhere, JOSEPH GARRISON, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit an offense against the United States, to wit, a violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(a)(4).

2. It was a part and an object of the conspiracy that JOSEPH GARRISON, the defendant, and others known and unknown, would and did intentionally access a computer without authorization, and exceed authorized access, and thereby would and did obtain information from a protected computer, which was committed for purposes of commercial advantage and private financial gain, and the value of the information obtained would and did exceed \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i) & (iii).

3. It was further a part and an object of the conspiracy that JOSEPH GARRISON, the defendant, and others known and unknown, knowingly and with the intent to defraud, would and did access a protected computer without authorization, and exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value

totaling more than \$5,000 during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A).

Overt Act

4. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt act, among others, was committed in the Southern District of New York and elsewhere:

a. On or about November 18, 2022, JOSEPH GARRISON, the defendant, used leaked credentials to access victims' electronic betting accounts on a fantasy sports and sports betting website (the "Betting Website").

(Title 18, United States Code, Section 371.)

COUNT TWO

(Computer Fraud - Unauthorized Access to a Protected Computer to Further Intended Fraud)

5. In or about November 2022, in the Southern District of New York and elsewhere, JOSEPH GARRISON, the defendant, knowingly and with the intent to defraud, accessed a protected computer without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained anything of value totaling more than \$5,000 during a one-year period, to wit, GARRISON obtained unauthorized access to victims' electronic betting accounts on the Betting Website and sold the means of unauthorized access to those accounts—namely, account login information along with instructions for how to drain funds from the compromised accounts—to others who used that information to steal hundreds of thousands of dollars from the victim accounts.

(Title 18, United States Code, Sections 1030(a)(4), 1030(c)(3)(A), and 2.)

COUNT THREE

(Computer Fraud - Unauthorized Access to a Protected Computer)

6. In or about November 2022, in the Southern District of New York and elsewhere, JOSEPH GARRISON, the defendant, intentionally accessed a computer without authorization, and exceeded authorized access, and thereby obtained information from a protected computer, which was committed for purposes of commercial advantage and private financial gain, and the value of the information obtained exceeded \$5,000, to wit, GARRISON obtained unauthorized access to victims' electronic betting accounts on the Betting Website and obtained information from those accounts, namely account login information, which he sold to others who used that information to steal hundreds of thousands of dollars from the victim accounts.

(Title 18, United States Code, Sections 1030(a)(2)(c), 1030(c)(2)(B)(i), and 2.)

COUNT FOUR
(Wire Fraud Conspiracy)

7. In or about November 2022, in the Southern District of New York and elsewhere, JOSEPH GARRISON, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

8. It was a part and an object of the conspiracy that JOSEPH GARRISON, the defendant, and others known and unknown, knowingly having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, GARRISON agreed with others to engage in a scheme to obtain unauthorized access to victims' electronic betting accounts on the Betting Website under false pretenses in order to steal hundreds of thousands of dollars from the victim accounts.

(Title 18, United States Code, Section 1349.)

COUNT FIVE
(Wire Fraud)

9. In or about November 2022, in the Southern District of New York and elsewhere, JOSEPH GARRISON, the defendant, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations and promises, transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, to wit, GARRISON engaged in a scheme to obtain unauthorized access to victims' electronic betting accounts on the Betting Website under false pretenses in order to steal hundreds of thousands of dollars from the victim accounts.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT SIX
(Aggravated Identity Theft)

10. In or about November 2022, in the Southern District of New York and elsewhere, JOSEPH GARRISON, the defendant, knowingly transferred, possessed, and used, without lawful authority, means of identification of another person, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, GARRISON transferred and used, and aided and abetted the use of, the identifying information of other people during and in

relation to the computer intrusion and wire fraud offenses charged in Counts One through Five of this Complaint.

(Title 18, United States Code, Sections 1028A(a)(1) and (b), and 2.)

The bases for my knowledge and the foregoing charges are, in part, as follows:

11. I am a Special Agent with the FBI. This affidavit is based on my personal participation in the investigation of this matter, my conversations with other law enforcement agents, witnesses and others, as well as my examination of reports and records. Because this affidavit is being submitted for the limited purpose of demonstrating probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

Overview

12. JOSEPH GARRISON, the defendant, launched a credential stuffing attack on the Betting Website in November 2022 (the “Betting Website Attack”) and thereby obtained access to tens of thousands of the Betting Website user accounts (the “Victim Accounts”).

13. During a credential stuffing attack, a cyber threat actor collects stolen credentials, or username and password pairs, obtained from other large-scale data breaches of other companies, which can be purchased on the darkweb.¹ The threat actor then systematically attempts to use those stolen credentials to obtain unauthorized access to accounts held by the same user with other companies and providers, in order to compromise accounts where the user has maintained the same password.²

14. GARRISON then sold access to those Victim Accounts through various websites that marketed and sold illegal account credentials. The buyers of those credentials accessed the Victim Accounts and withdrew approximately \$600,000 in total from the Victim Accounts.

15. Law enforcement identified JOSEPH GARRISON, the defendant, as the individual who conducted the Betting Website Attack based on the following, in substance and in part:

¹ Darkweb marketplaces are underground e-commerce websites that offer contraband over the Internet. These marketplaces use technology, including The Onion Router or “Tor” network, and cryptocurrency, to protect the anonymity of the individuals that operate the marketplace, as well as the vendors and customers who use the marketplace.

² To give an example of how a credential stuffing attack might work, an individual might purchase a list of 100,000 usernames and passwords obtained from a hack or data breach of an email service provider, and then use a computer program to rapidly attempt to log into financial accounts using each of those 100,000 linked usernames and passwords.

a. When law enforcement began its investigation, credentials stolen in the Betting Website Attack were being offered for sale on the internet. Undercover law enforcement purchased certain credentials stolen in the Betting Website Attack, and the Internet protocol (“IP”) address³ that uploaded the instructions to use those stolen credentials to steal money from the Victim Accounts was linked to GARRISON.

b. Law enforcement executed a search on GARRISON’s home, where they recovered, among other things: (i) credential stuffing programs and files establishing that GARRISON used those programs to access the Betting Website; (ii) instructional photographs about how to use the stolen credentials to steal money from the Victim Accounts; (iii) messages between GARRISON and co-conspirators about the Betting Website Attack; and (iv) messages from GARRISON to co-conspirators about other similar credential stuffing attacks, including but not limited to the message, “fraud is fun,” which referred to credential stuffing attacks generally.

c. Prior to the Betting Website Attack, in an interview conducted by the Madison, Wisconsin Police Department, GARRISON admitted to participating in similar credential stuffing attacks.

The Credential Stuffing Attack on the Betting Website

16. Based on law enforcement communications with employees of the Betting Website and my review of records provided by the Betting Website, I have learned the following, in substance and in part:

a. The Betting Website is a fantasy sports and sports betting company.

b. On or about November 18, 2022, the Betting Website was subjected to a credential stuffing attack (*i.e.*, the Betting Website Attack). In connection with the Betting Website Attack, there was a series of attempts to log into the Betting Website accounts using a large list of credentials.

c. I further know from my training and experience that when individuals successfully execute a credential stuffing attack, they will frequently sell access to many of the accounts they have illegally accessed on various websites that deal in hacked accounts.

d. In connection with the Betting Website Attack on or about November 18, 2022, approximately 60,000 Victim Accounts at the Betting Website were successfully compromised.

e. In some instances, the individuals who unlawfully accessed the Victim Accounts were able to add a new payment method on the account, deposit \$5 into that

³ An IP address is a unique numeric address used by internet-enabled electronic storage devices. Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination.

account through the new payment method to verify that method, and then withdraw all the existing funds in the Victim Account through the new payment method (*i.e.*, to a newly added financial account belonging to the hacker), thus stealing the funds in the Victim Account. Using this method, the hackers stole approximately \$600,000 from approximately 1,600 Victim Accounts.

17. Based on my review of records provided by the Betting Website, I have learned, in substance and in part, that at least 30 of the 60,000 Victim Accounts accessed via the Betting Website Attack have listed addresses in the Southern District of New York. I have additionally interviewed approximately four individuals who confirmed that they were victims of the Betting Website Attack and that they reside in the Southern District of New York.

Undercover Purchases of the Betting Website Credentials and IP Address Analysis

18. Based on discussions with employees of the Betting Website and an undercover law enforcement officer (the “UC”), as well as my review of records relating to an undercover operation, I have learned the following, in substance and in part:

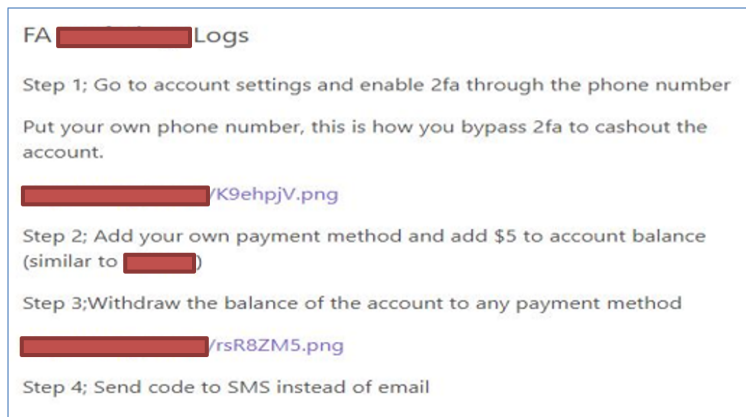
a. In approximately November 2022, the Betting Website informed law enforcement that working Betting Website credentials, verified through the Betting Website, were available for purchase on several illicit websites.

b. The Betting Website further informed law enforcement that Betting Website representatives purchased stolen credentials after the Betting Website Attack in an attempt to investigate the hack. When the Betting Website made that purchase, it received instructions as to how to steal money from the purchased Victim Accounts. Those instructions contained several photos of a particular Victim Account as an illustration (the “Illustration Account”). The Betting Website checked the status of the Illustration Account on its own systems and saw that money had been withdrawn from the account on or about November 18, 2022, in a manner consistent with the hacking instructions. The Betting Website observed that a particular IP address was used to access the Illustration Account and withdraw the money on or about November 18, 2022 (the “Target IP Address”).

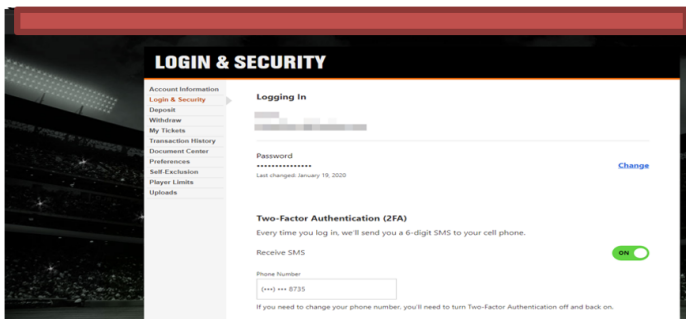
c. On or about January 9, 2023, the UC observed stolen Betting Website credentials for sale on a website (“Website-1”). The UC purchased two sets of those credentials—meaning usernames and passwords for two Victim Accounts—for approximately \$11 (the “Website-1 Credentials”). The UC made the purchase of credentials from an office located in the Southern District of New York and the credentials were transmitted to the UC and downloaded by the UC from the office located in the Southern District of New York. Law enforcement confirmed with the Betting Website that the email addresses in the Website-1 Credentials belonged to active Betting Website accounts.

d. When the UC purchased the Website-1 Credentials, the seller who had sold those credentials on Website-1 provided instructions as to how the Website-1 Credentials could be used to steal money from the Victim Accounts. Those instructions are below:⁴

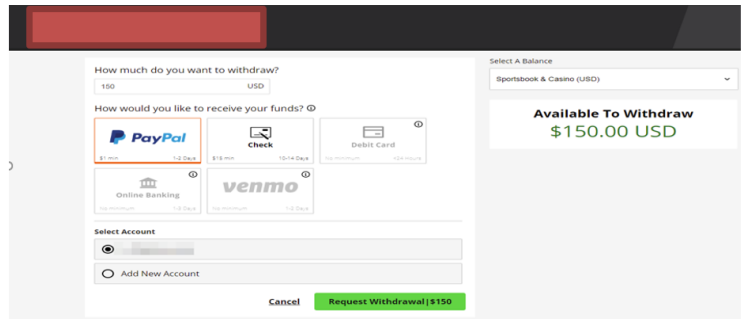
⁴ Certain of the pictures in this Complaint have been redacted to protect identities.



e. The instructions provided through Website-1 included links (the hyperlinks in the photo above) to two photos of money being extracted from the Illustration Account with additional instructions, and those photos with additional instructions were hosted on an image hosting website (the “Hosting Website”). The two photos hosted at the Hosting Website links are below:⁵



[Hosting Website domain omitted]/K9ehpjV.png
 (“Photo-1”)



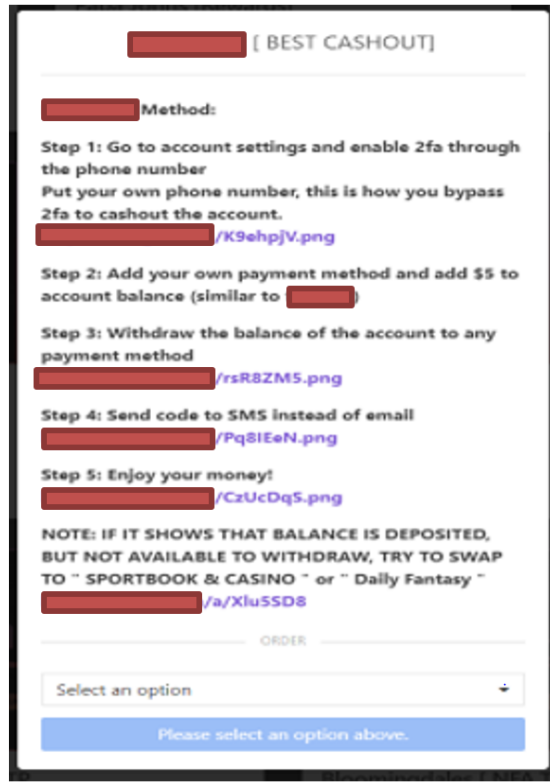
[Hosting Website domain omitted]/rsR8ZM5.png
 (“Photo-2”)

19. I have reviewed information provided by the Hosting Website identifying the IP addresses that uploaded Photo-1 and Photo-2 to the Hosting Website. Different IP addresses uploaded Photo-1 and Photo-2. The IP address that uploaded Photo-2 was the Target IP Address, and Photo-2 was uploaded on or about November 18, 2022.

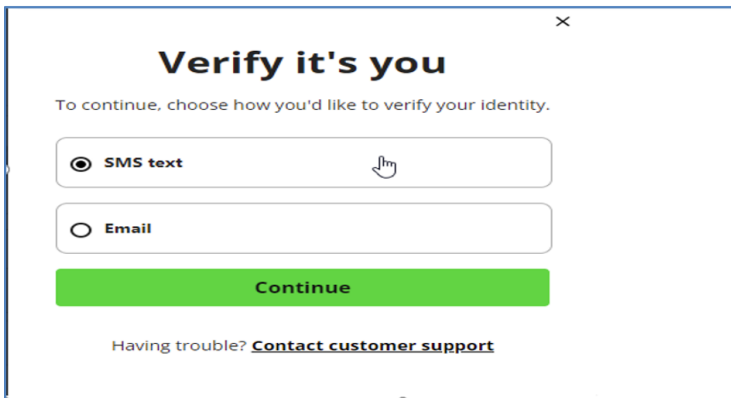
20. Law enforcement observed that stolen Betting Website credentials were also available for purchase on another website (“Website-2”).

21. While law enforcement did not purchase Betting Website credentials from Website-2, they observed the following instructions on Website-2 as to how to use any purchased Betting Website credentials to steal money:

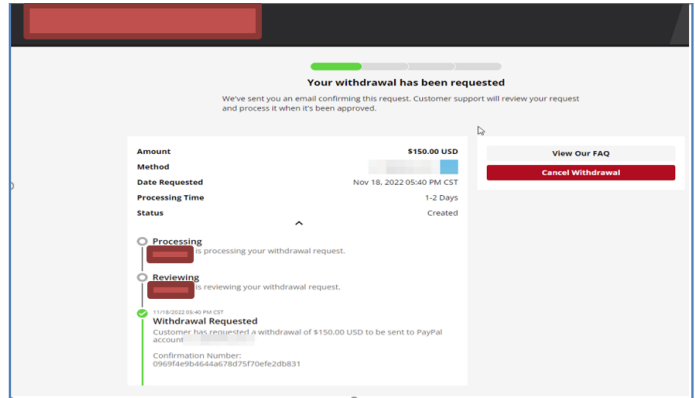
⁵ The Hosting Website links described in this warrant are no longer working, and law enforcement used the database service the Internet Archive to view the photos at the Hosting Website links.



22. Similar to the instructions from Website-1 shown above in paragraph 18, the instructions from Website-2 contain several Hosting Website links showing exactly how to take various steps to steal money from the Victim Accounts. The first Hosting Website link in the Website-2 instructions is a link to Photo-1. The second Hosting Website link in the Website-2 instructions is a link to Photo-2, which, as described above, was uploaded using the Target IP Address. The pictures from the third and fourth Hosting Website links in the Website-2 instructions are below:



[Hosting Website domain omitted]/Pq8IEeN.png
("Photo-3")



[Hosting Website domain omitted]/CzUcDqS.png
("Photo-4")

23. I have reviewed information provided by the Hosting Website identifying the IP addresses that uploaded Photo-3 and Photo-4 to the Hosting Website. The Target IP Address

uploaded both Photo-3 and Photo-4 on or about November 18, 2022—which is the same date that Photo-2 was uploaded using the Target IP Address, and the same date that funds were withdrawn from the Illustration Account using the Target IP Address.

24. I have reviewed a subpoena return from the provider of the Target IP Address. The subscribers of the Target IP Address are the parents of JOSEPH GARRISON, the defendant, and the physical address is a location in Wisconsin (the “Wisconsin Address”). The subpoena return further established that the Wisconsin Address had used the Target IP Address from approximately September 29, 2022 until at least approximately January 30, 2023, during which time Photo-2, Photo-3, and Photo-4 were uploaded to the Hosting Website.

The Search of GARRISON’s Home

25. I know from my involvement in the investigation that on or about February 23, 2023, law enforcement executed a search at the Wisconsin Address pursuant to a judicially authorized search warrant. JOSEPH GARRISON, the defendant, and his family reside at the Wisconsin Address. In that search, law enforcement recovered and searched several devices belonging to GARRISON, including his computer (the “Garrison Computer”) and cellphone (the “Garrison Phone”).

Credential Stuffing Tools on the Garrison Computer

26. I know from my involvement in the investigation that law enforcement located the programs OpenBullet and SilverBullet on the Garrison Computer. Based on my involvement in the investigation and my training and experience, I know the following about OpenBullet, SilverBullet, and the files found on the Garrison Computer, in substance and in part:

a. OpenBullet and SilverBullet are programs frequently used to execute credential stuffing attacks.

b. To launch a credential stuffing attack using OpenBullet or SilverBullet, an individual needs both a “wordlist” and a “config.” A “wordlist” contains a series of username and password combinations, while a “config” is a script that will run the wordlist through the log-in page of a particular website.

c. On the Garrison Computer, law enforcement located 11 separate Betting Website configs. Metadata shows that the earliest creation date for one of those configs was November 17, 2022, approximately one day before the Betting Website Attack.

d. On the Garrison Computer, law enforcement also located approximately 700 separate configs designed for credential stuffing attacks against dozens of other company websites.

e. On the Garrison Computer, law enforcement located at least 69 wordlists which contained at least 38,484,088 individual username and password combinations.⁶

Additional Files Related to the Betting Website Attack

27. On the Garrison Computer, law enforcement also located Photo-1, Photo-2, Photo-3, and Photo-4, which, as described above, contained the instructions for individuals who purchased Betting Website credentials to use those credentials to steal money. Those photos were created using a particular program that: (a) indicated that JOSEPH GARRISON, the defendant, had created the photos; and (b) indicated that the photos had been created on or about November 18, 2022, the date of the Betting Website Attack.

GARRISON's Messages About the Betting Website Attack

28. On the Garrison Phone, law enforcement located the following chats with a co-conspirator about the Betting Website Attack ("CC-1"). Based on my training and experience and involvement in the investigation, I believe that JOSEPH GARRISON, the defendant, and CC-1 were discussing, among other things, how to execute the Betting Website Attack and how to profit from the Betting Website Attack by extracting funds from the Victim Accounts directly or by selling access to the Victim Accounts:

Date	From	Message
11/17/2022	GARRISON	do u have captcha ⁷
11/17/2022	CC-1	uh
11/17/2022	CC-1	not rly
11/17/2022	CC-1	for what site u need
11/17/2022	GARRISON	[the Betting Website]
11/17/2022	CC-1	eh
11/17/2022	CC-1	its shit
11/17/2022	CC-1	don't bother
11/17/2022	GARRISON	i have bypass ⁸
11/17/2022	CC-1	2fa? ⁹

⁶ Some of these combinations are likely duplicates.

⁷ Based on my training and experience and involvement in the investigation, I understand "captcha" to be an acronym for "Completely Automated Public Turing test to tell Computers and Humans Apart," a verification tool at the log-in stage in which a human must correctly identify, for example, altered text in a picture, to ensure that a bot is not attempting to log in. Successful credential stuffing attacks frequently rely on overcoming CAPTCHA protections.

⁸ Based on my training and experience and involvement in the investigation, I understand "bypass" to refer to a method to avoid anti-hacking protocols by websites, such as two-factor authentication and CAPTCHAs.

⁹ Based on my training and experience and involvement in the investigation, I understand "2fa" to refer to "two-factor authentication," a protocol to make hacking accounts more difficult.

11/17/2022	CC-1	[name of coconspirator omitted]
11/17/2022	CC-1	bypass
11/17/2022	CC-1	jeez
11/17/2022	CC-1	u rich
[]		
11/18/2022	GARRISON	if u get captcha
11/18/2022	GARRISON	we can do
11/18/2022	GARRISON	[the Betting Website]
11/18/2022	GARRISON	too
11/18/2022	CC-1	i have solver
11/18/2022	CC-1	it's just
11/18/2022	CC-1	[the Betting Website]
11/18/2022	CC-1	doesn't hit
11/18/2022	CC-1	for me
11/18/2022	GARRISON	u need bypass
11/18/2022	GARRISON	i have it
[]		
11/18/2022	GARRISON	[Messaged lines of code that I understand, from my training and experience and involvement in the investigation, are designed to be used against the Betting Website]
[]		
11/18/2022	GARRISON	[name of coconspirator omitted] got like
11/18/2022	GARRISON	20k worth of accs ¹⁰
11/18/2022	GARRISON	In like 3hrs checking
11/18/2022	CC-1	Imma get more
11/18/2022	GARRISON	Give me bulk ill sell on other shops ¹¹
11/18/2022	GARRISON	I have a bunch lined up
11/18/2022	GARRISON	Ill give u profit
[]		
11/18/2022	CC-1	[Messages a photo of SilverBullet running against the Betting Website]
[]		
11/18/2022	GARRISON	wanna toss me a hit so i can write up method
11/18/2022	GARRISON	make it all pretty for ur customers
11/18/2022	GARRISON	and easy to understand
11/18/2022	CC-1	[username omitted] [password omitted] Balance = \$150.00 [username omitted] [password omitted] Balance = \$100.00

¹⁰ Based on my training and experience and involvement in the investigation, I understand “accs” to be short for “accounts,” and to refer to individual user accounts that have been successfully illegally accessed.

¹¹ Based on my training and experience and involvement in the investigation, I understand terms like “shop” and “acc shop” to refer in this context to websites such as Website-1 and Website-2, that sell stolen log-in credentials.

		[username omitted] [password omitted] Balance = \$250.00
11/18/2022	CC-1	here u go my brotha
11/18/2022	CC-1	u will give me method?
11/18/2022	CC-1	lol
11/18/2022	GARRISON	ye
11/18/2022	CC-1	i will give u 30% of all
[]		
11/18/2022	GARRISON	<p>[the Betting Website] Method</p> <p>Step 1; Go to account settings and enable 2fa through the phone number</p> <p>Put your own phone number, this is how you bypass 2fa to cashout the account.</p> <p>[Hosting Website domain omitted]/K9ehpjV.png</p> <p>Step 2; Add your own payment method and add \$5 to account balance (similar to [name of other fantasy sports and sports betting website omitted])</p> <p>Step 3; Withdraw the balance of the account to any payment method</p> <p>[Hosting Website domain omitted]/rsR8ZM5.png</p> <p>Step 4; Send code to SMS instead of email</p> <p>[Hosting Website domain omitted]/Pq8IEeN.png</p> <p>Step 5; Enjoy your money!</p> <p>[Hosting Website domain omitted]/CzUcDqS.png</p>
[]		
11/18/2022	CC-1	1k accs
11/18/2022	CC-1	with \$100+
11/18/2022	GARRISON	[Messaged file that I understand, from my training and experience and involvement in the investigation, to be a config file to run against the Betting Website]
11/18/2022	GARRISON	all the shop owners will buy an acc from u too to get method
[]		
11/18/2022	CC-1	gogo
11/18/2022	CC-1	[username omitted] [password omitted] Balance = \$12,636.14
11/18/2022	GARRISON	i needa find a drop ¹²
[]		
11/19/2022	GARRISON	[Messages a photo of a search on Twitter for “[the Betting Website] hacked”]

29. On the Garrison Phone, law enforcement also located the following chats with a second co-conspirator about the Betting Website Attack (“CC-2”). Based on my training and experience and involvement in the investigation, I believe that JOSEPH GARRISON, the

¹² Based on my training and experience and involvement in the investigation, I understand a “drop” to refer to a bank account that can be used to deposit hacked funds.

defendant, and CC-2 were discussing, among other things, how GARRISON would provide access to stolen credentials that CC-2 would then arrange to resell:

Date	From	Message
11/18/2022	GARRISON	hi
11/18/2022	GARRISON	i got
11/18/2022	GARRISON	[the Betting Website]
11/18/2022	CC-2	No captcha ?
11/18/2022	GARRISON	i have captchaless vm
11/18/2022	GARRISON	i can stock u if u want
11/18/2022	CC-2	Yesss pls
11/18/2022	CC-2	I have method
11/18/2022	CC-2	And all
11/18/2022	GARRISON	i made the method
11/18/2022	GARRISON	[The Betting Website] Method Step 1; Go to account settings and enable 2fa through the phone number Put your own phone number, this is how you bypass 2fa to cashout the account. [Hosting Website domain omitted]/K9ehpjV.png Step 2; Add your own payment method and add \$5 to account balance (similar to [name of other fantasy sports and sports betting website omitted]) Step 3; Withdraw the balance of the account to any payment method [Hosting Website domain omitted]/rsR8ZM5.png Step 4; Send code to SMS instead of email [Hosting Website domain omitted]/Pq8IEeN.png Step 5; Enjoy your money! [Hosting Website domain omitted]/CzUcDqS.png
11/18/2022	GARRISON	ima take my dog out then ill stock u
11/18/2022	GARRISON	i got a fuck ton of stock
11/18/2022	CC-2	Okay bet
11/18/2022	CC-2	And I can show full stats of what's sold cuz of my custom site
11/18/2022	CC-2	#stats op
11/18/2022	GARRISON	lmao
11/18/2022	GARRISON	lemme sort this shit
11/18/2022	CC-2	Damn I jus realized this the same method I did wit [name of other fantasy sports and sports betting website omitted]
[]		
11/18/2022	GARRISON	[Messages picture showing that he has 175 Victim Accounts with between \$25-\$50, 67 Victim Accounts with between \$50-\$99, 45 Victim Accounts with between \$100-\$150, 15 accounts with between \$150-\$200, 18 Victim Accounts with between \$200-\$400, 10 Victim Accounts with between \$500-\$999, and 8 Victim Accounts with more than \$1,000]

11/18/2022	GARRISON	ill add up total value
		□
11/18/2022	GARRISON	\$31k
11/18/2022	GARRISON	of accs

GARRISON's Messages About Other Computer Frauds

30. On the Garrison Phone, law enforcement also located the following chats with a third co-conspirator ("CC-3") about additional hacking by JOSEPH GARRISON, the defendant, which were exchanged approximately two months before the Betting Website Attack. Based on my training and experience and involvement in the investigation, I understand that JOSEPH GARRISON, the defendant, and CC-3 were discussing, among other things, that GARRISON was successful at credential stuffing attacks, that GARRISON enjoyed credential stuffing attacks, and GARRISON's belief that law enforcement would not catch or prosecute him for his credential stuffing attacks:

Date	From	Message
9/14/2022	GARRISON	i quit simming ¹³
9/14/2022	GARRISON	im back to cracking ¹⁴
9/14/2022	GARRISON	im getting sites no1 has had for like ever and shit
9/14/2022	GARRISON	i have every captcha bypassed
		□
9/16/2022	GARRISON	fraud is fun
9/16/2022	GARRISON	im addicted to see money in my account
9/16/2022	CC-3	idk it ruined my life personally
		□
9/16/2022	GARRISON	idk im like obsessed with bypassing shit
		□
9/16/2022	GARRISON	im thinking of starting a shop myself
9/16/2022	CC-3	i wouldn't lol
9/16/2022	CC-3	u already under enough heat
9/16/2022	CC-3	And already made 6 figures in an afternoon
		□
9/16/2022	GARRISON	i couldbe in every big shops tele
9/16/2022	GARRISON	[CC-3] at some point u gotta realize
9/16/2022	GARRISON	no1 cares ab
9/16/2022	GARRISON	acc shops

¹³ Based on my training and experience and involvement in the investigation, I understand "simming," or "sim swapping," to refer to a scam in which a victim's phone number is ported over to a cellphone SIM card controlled by the criminal, thus allowing the criminal to circumvent two-factor authentication protocols by intercepting verification calls and text messages.

¹⁴ Based on my training and experience and involve in the investigation, I understand "cracking" to refer to credential stuffing.

9/16/2022	GARRISON	theyd care if I sold cp ¹⁵ on it
-----------	----------	---------------------------------------------

31. On the Garrison Phone, law enforcement located the following chats with a coconspirator (“CC-4”) about additional hacking by JOSEPH GARRISON, the defendant:

Date	From	Message
10/26/2022	GARRISON	I haven’t been focusing on
10/26/2022	GARRISON	accs
10/26/2022	GARRISON	I do a lot of other types of fraud

The June 2022 Interview of GARRISON

32. I have reviewed a written report by the Madison, Wisconsin Police Department about a non-custodial interview of JOSEPH GARRISON, the defendant, on or about June 14, 2022 (approximately five months before the Betting Website Attack). Law enforcement began the interview of GARRISON at the Wisconsin Address and then continued it at a police station. During the interview, GARRISON, stated the following, in substance and in part:

a. GARRISON previously ran a website called “Goat Shop” on which individuals sold hacked accounts.

b. GARRISON himself hacked accounts and then sold them on Goat Shop.

c. GARRISON described the way that he hacked accounts, namely that he had taken username and passwords from data breaches, put them into a program called “Open Bullet,” and then used Open Bullet to attempt to access other websites using those lists of usernames and passwords. GARRISON used the term “credential stuffing” to describe these previous hacks.

d. GARRISON hacked accounts and then sold access to the hacked accounts on Goat Shop from approximately 2018 through approximately 2021, he made approximately \$15,000 per day from the website at its peak, and he had made approximately \$800,000 in total.

e. GARRISON had stopped the hacking activity in or about the end of 2021. As set forth in this Complaint, this statement was false.

33. On the Garrison Phone, law enforcement located an undated picture showing that Goat Shop had sold 225,247 products for total sales revenue of \$2,135,150.09.

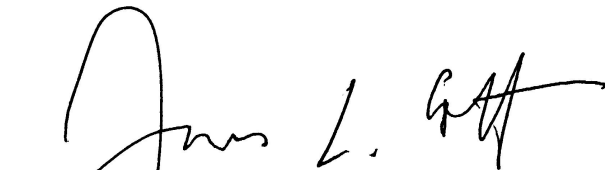
¹⁵ Based on my training and experience and involve in the investigation, I understand “cp” to be an abbreviation for child pornography.

WHEREFORE, the deponent respectfully requests that a warrant be issued for the arrest of JOSEPH GARRISON, the defendant, and that he be arrested and imprisoned, or bailed, as the case may be.

/s/ Michael Gassert, by the Court, with permission

MICHAEL GASSERT
Special Agent
Federal Bureau of Investigation

Sworn to me through the transmission
of this Complaint by reliable electronic
means, pursuant to Federal Rules of
Criminal Procedure 41(d)(3) and 4.1, this
15th day of May, 2023



JAMES L. COTT
United States Magistrate Judge